UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/511,775	05/16/2005	John Heasman	FLWH.P-001	6608

57380 7590 10/14/2009

Oppedahl Patent Law Firm LLC
P O Box 5940
Dillon, CO 80435-5940

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
10/14/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket-oppedahl@oppedahl.com

Office Action Summary	Application No.	Applicant(s)	
	10/511,775	HEASMAN ET AL.	
	Examiner	Art Unit	
	ARAVIND K. MOORTHY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9 and 10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9 and 10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 October 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 3 August 2009.

2. Claims 1-7, 9 and 10 are pending in the application.

3. Claims 1-7, 9 and 10 have been rejected.

4. Claim 8 has been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3 August 2009 has been entered.

Response to Amendment

6. The examiner approves of the amendment made to the specification. No new matter has been added.

Response to Arguments

7. Applicant's arguments with respect to claims 1-7, 9 and 10 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an

international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 2 and 6 are rejected under 35 U.S.C. 102(e) as being anticipated by Pearson U.S. Patent No. 6,990,591 B1.

As to claim 1, Pearson discloses an intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network, the network intrusion detection system comprising:

Pearson discloses the intrusion detection system comprising means for monitoring activity relative to the computer system or network (i.e. Computer 102, LAN 104, and server 105 are typically connected to the Internet 108 through a communication device 106 such as gateway, firewall, or other device that communicates data between one or more ports. According to an exemplary embodiment of the present invention, communication device 106 comprises a network firewall intrusion detection appliance that is further described with reference to FIG. 2 below. The firewall and intrusion detection functionality of communication device 106 protects the resources of LAN 104 from potential hackers, such as renegade users of the Internet 108 or unauthorized users of LAN 104, by monitoring the communications received into the device 106 and determining whether such communications comprise a security risk. The general operation of the firewall and intrusion detection functionality is described below with reference to FIG. 2.) [column 6, lines 5-20];

Pearson disclose means for receiving and storing one or more general rules. Pearson discloses that each of the general rules being representative of the

effect on the computer system or network arising from plurality of specific instances of intrusion or attempted intrusion (i.e. In addition to firewall functionality, the preferred communication device 106 implements intrusion detection functionality via intrusion detector 160, by monitoring the communications received into communication device 106 and determining whether such communications comprise an attack or other security risk. More particularly, intrusion detector 160 inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list 170 of known attack signatures. Attack signatures are activity patterns indicative of undesirable activity, i.e., evidence that an unauthorized communication has been received. Examples of attacks include Denial of Service (DoS) attacks, unauthorized access attacks, attempts to modify data or kill programs, protocol violations, and repeated access attempts indicating malicious intent. Representative examples of attack signatures are shown in FIG. 9 and will be further described below with reference to that figure. Intrusion detector 160 may also monitor for attacks by users that are authorized to be on LAN 104. Therefore, any attack or unauthorized activity on the network can be detected and the RMC 130 is automatically notified by an alert signal transmitted by the RMC communications module 165.) [column 8, lines 10-32].

Pearson discloses matching means for receiving data relating to activity relative to the computer system or network from the monitoring means and for comparing, in a semantic manner, sets of actions forming the activity against the

one or more general rules to identify an intrusion or attempted intrusion (i.e. Method 700 begins at step 702, where an activated and remotely monitored communication device 106 receives a communication, for example from a hacker 150 (FIG. 1). This communication may constitute a threat or attack to the user's network, or may merely constitute a desired communication. Method 700 continues to step 704, where the received communication is compared to a list of known attacks and the result of the comparison is provided to a decision block 706. Preferably, all received communications are analyzed and compared to the list of known attacks. As described above with reference to FIG. 4B, a received communication will generally constitute a security risk if the type of communication received matches a communication type on the predetermined list 170 of communication types deemed to be attacks.) [column 16, lines 35-49].

As to claim 2, Pearson discloses that the one or more general rules forms a knowledge base of the system (i.e. The function of intrusion detection is well known to those skilled in the art. Typically, an intrusion detection function is carried out in software, and can be implemented in software, hardwire, or firmware. Typically, intrusion detection is carried out by comparing an incoming communication (usually comprising a string of characters embedded within a TCP/IP packet, such characters being provided by another computer or a user of another computer that is requesting services) to a list of known attack signatures stored in an attack signature list 170. The attack signature list is preferably stored in a rewritable memory within the communication device 106 so that the list can be updated as new attack signatures are identified.) [column 8, lines 33-45].

As to claim 6, Pearson discloses an intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network, the intrusion detection system comprising:

Pearson discloses the intrusion detection system comprising means for monitoring activity relative to the computer system or network (i.e. Computer 102, LAN 104, and server 105 are typically connected to the Internet 108 through a communication device 106 such as gateway, firewall, or other device that communicates data between one or more ports. According to an exemplary embodiment of the present invention, communication device 106 comprises a network firewall intrusion detection appliance that is further described with reference to FIG. 2 below. The firewall and intrusion detection functionality of communication device 106 protects the resources of LAN 104 from potential hackers, such as renegade users of the Internet 108 or unauthorized users of LAN 104, by monitoring the communications received into the device 106 and determining whether such communications comprise a security risk. The general operation of the firewall and intrusion detection functionality is described below with reference to FIG. 2.) [column 6, lines 5-20].

Pearson discloses means for initially receiving and storing a knowledge base comprising one or more general rules. Pearson discloses that each of the general rules being representative of characteristics associated with a plurality of specific instances of intrusion or attempted intrusion (i.e. In addition to firewall functionality, the preferred communication device 106 implements intrusion

detection functionality via intrusion detector 160, by monitoring the communications received into communication device 106 and determining whether such communications comprise an attack or other security risk. More particularly, intrusion detector 160 inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list 170 of known attack signatures. Attack signatures are activity patterns indicative of undesirable activity, i.e., evidence that an unauthorized communication has been received. Examples of attacks include Denial of Service (DoS) attacks, unauthorized access attacks, attempts to modify data or kill programs, protocol violations, and repeated access attempts indicating malicious intent. Representative examples of attack signatures are shown in FIG. 9 and will be further described below with reference to that figure. Intrusion detector 160 may also monitor for attacks by users that are authorized to be on LAN 104. Therefore, any attack or unauthorized activity on the network can be detected and the RMC 130 is automatically notified by an alert signal transmitted by the RMC communications module 165.) [column 8, lines 10-32].

Pearson discloses means for automatically generating and storing in the knowledge base (i.e. Method 700 begins at step 702, where an activated and remotely monitored communication device 106 receives a communication, for example from a hacker 150 (FIG. 1). This communication may constitute a threat or attack to the user's network, or may merely constitute a desired communication. Method 700 continues to step 704, where the received

communication is compared to a list of known attacks and the result of the comparison is provided to a decision block 706. Preferably, all received communications are analyzed and compared to the list of known attacks. As described above with reference to FIG. 4B, a received communication will generally constitute a security risk if the type of communication received matches a communication type on the predetermined list 170 of communication types deemed to be attacks.) [column 16, lines 35-49].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 3-5, 7, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pearson U.S. Patent No. 6,990,591 B1 in view of "Applications of Inductive Logic Programming" (hereinafter Bratko).

As to claim 3, Pearson discloses if no session entry is found in step 102, a new session entry is created in the session cache 44 in step 106. Session data, which includes any matches identified by executing attack signature profile instructions on a data packet, are entered into the new session entry in step 108 and the session entry is entered into the state cache 44 in step 110 [column 9, lines 21-27].

Pearson does not teach that the means for automatically generating and storing a new general rule (i.e. new session entry) comprises inductive logic programming means.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson so that the means for generating and storing a new rule (i.e. updated rules) would have been done by using inductive logic programming.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

As to claims 4, 9 and 10, Pearson discloses that in step 56 the communication module 30 of the data repository 12 distributes the signature profiles to the various data collectors 10 throughout the network. Upon receiving a set or sets of attack signature profiles, each data collector 10 stores the set or sets of profiles it receives from the data repository 12 in its signature profile memory 39 [column 6, lines 50-56].

Pearson does not teach that the one or more general rules is or are represented in a logic programming language.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson so that the rules as taught would have been represented by inductive logic programming.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

As to claim 5, Pearson discloses that multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions [column 5, lines 26].

Pearson does not teach that inductive logic programming techniques are applied by the system to an attack an intrusion or attempted intrusion.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson so that the rules of an attack would have been applied by inductive logic programming to derive positive examples.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

As to claim 7, Pearson discloses an intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network, the intrusion detection system comprising:

> Pearson discloses the intrusion detection system comprising means for monitoring activity relative to the computer system or network (i.e. Computer 102, LAN 104, and server 105 are typically connected to the Internet 108 through a communication device 106 such as gateway, firewall, or other device that

communicates data between one or more ports. According to an exemplary embodiment of the present invention, communication device 106 comprises a network firewall intrusion detection appliance that is further described with reference to FIG. 2 below. The firewall and intrusion detection functionality of communication device 106 protects the resources of LAN 104 from potential hackers, such as renegade users of the Internet 108 or unauthorized users of LAN 104, by monitoring the communications received into the device 106 and determining whether such communications comprise a security risk. The general operation of the firewall and intrusion detection functionality is described below with reference to FIG. 2.) [column 6, lines 5-20].

Pearson discloses means for initially receiving and storing in a knowledge base data representative of the effect on the computer system or network arising from one or more specific instances or classes of intrusion or attempted intrusion. (i.e. In addition to firewall functionality, the preferred communication device 106 implements intrusion detection functionality via intrusion detector 160, by monitoring the communications received into communication device 106 and determining whether such communications comprise an attack or other security risk. More particularly, intrusion detector 160 inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list 170 of known attack signatures. Attack signatures are activity patterns indicative of undesirable activity, i.e., evidence that an unauthorized communication has been received.

Examples of attacks include Denial of Service (DoS) attacks, unauthorized access attacks, attempts to modify data or kill programs, protocol violations, and repeated access attempts indicating malicious intent. Representative examples of attack signatures are shown in FIG. 9 and will be further described below with reference to that figure. Intrusion detector 160 may also monitor for attacks by users that are authorized to be on LAN 104. Therefore, any attack or unauthorized activity on the network can be detected and the RMC 130 is automatically notified by an alert signal transmitted by the RMC communications module 165.) [column 8, lines 10-32].

Pearson discloses matching means for receiving data relating to activity relative to the computer system or network from the monitoring means and for comparing sets of actions forming the activity against the stored data to identify an intrusion or attempted intrusion (i.e. Method 700 begins at step 702, where an activated and remotely monitored communication device 106 receives a communication, for example from a hacker 150 (FIG. 1). This communication may constitute a threat or attack to the user's network, or may merely constitute a desired communication. Method 700 continues to step 704, where the received communication is compared to a list of known attacks and the result of the comparison is provided to a decision block 706. Preferably, all received communications are analyzed and compared to the list of known attacks. As described above with reference to FIG. 4B, a received communication will generally constitute a security risk if the type of communication received matches

a communication type on the predetermined list 170 of communication types deemed to be attacks.) [column 16, lines 35-49].

Pearson does not teach that the updating means include inductive logic programming means for updating the stored data to take into account the effect on the computer system or network arising from further instances or classes of intrusion or attempted intrusion occurring after the knowledge base has been initially received and stored.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson so that the updating means of the rules would have been done using inductive logic programming.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pearson by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431